UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/705,782	11/10/2003	Andrew Dellow	851963.414	4386

38106 7590 03/23/2009

SEED INTELLECTUAL PROPERTY LAW GROUP PLLC
701 FIFTH AVENUE, SUITE 5400
SEATTLE, WA 98104-7092

EXAMINER	
DEBNATH, SUMAN	
ART UNIT	**PAPER NUMBER**
2435	
MAIL DATE	**DELIVERY MODE**
03/23/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/705,782	DELLOW ET AL.	
	Examiner	Art Unit	
	SUMAN DEBNATH	2435	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *23 December 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-21* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-21* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-21 are pending in this application.

2. Claims 1, 10, 13, 16 and 19 are currently amended.

3. The text of these sections of Title 35, U.S. Code not included in this action can be found in a prior Office Action.

Claim Rejections - 35 USC § 103

4. Claims 1-21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Chaney (Patent No.: US 5,852,290) and further in view of Mills (Patent No.: US 6,311,204 B1).

5. As to claim 1, Chaney discloses a semiconductor integrated circuit, provided as a monolithic circuit, for decryption of broadcast signals, comprising:

an input interface for receipt of received encrypted broadcast signals and control data, and an output interface for output of decrypted broadcast signals (col. 3, lines 57-67 to col. 4, lines 1-5, col. 1, lines 59-67, col. 5, lines 25-67);

a processing unit arranged to receive encrypted broadcast signals via the input interface, to decrypt the encrypted broadcast signals in accordance with control signals, and to provide decrypted broadcast signals to the output interface (col. 5, lines 25-67);

a first decryption circuit arranged to receive encrypted control signals from the input interface and to decrypt the control signals in accordance with a common key from a common key store in the integrated circuit (col. 5, lines 25-67 and col. 6, lines 55-67);

Although Chaney discloses a second decryption circuit arranged to decrypt the control signals (col. 5, lines 25-67) and a common key store (col. 6, lines 65-67), Chaney doesn't explicitly disclose:

a second decryption circuit arranged to receive the common key in encrypted form from the input interface and to decrypt the common key in accordance with a secret key from a secret key store in the integrated circuit;

whereby the circuit is arranged such that the only route to placing a common key in the common key store is to input the common key in encrypted form for decryption in accordance with the secret key and provide the common key to the common key store over an internal bus, and the only route to providing the control signals to the processing unit is to input them in encrypted form for decryption in accordance with the common key.

However, Mills discloses a second decryption circuit arranged to receive the common key in encrypted form from the input interface and to decrypt the common key in accordance with a secret key from a secret key store (col. 11, lines 43-45);

whereby the circuit is arranged such that the only route to placing a common key in the common key store is to input the common key in encrypted form for decryption in accordance with the secret key and provide the common key to the common key store over an internal bus, and the only route to providing the control signals to the processing unit is to input them in encrypted form for decryption in accordance with the common key (col. 11, lines 30-50).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Chaney as taught y Mills in order to increase the security of broadcasted data that transmitted over the public network.

6. As to claims 10, 13, 16 and 19, these are rejected using the same rationale as for the rejection of claim 1.

7. As to claim 2, Chaney discloses wherein the first decryption circuit and second decryption circuit are formed in a common circuit (col. 5, lines 25-67).

8. As to claim 3, neither Chaney nor Mills explicitly discloses wherein at least one of the first decryption circuit and the second decryption circuit comprises an AES circuit. However, AES is a well known block ciphering which has been around for long time. It would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Chaney to utilize AES circuit for decrypting encrypted broadcast signal to take advantage of AES's recognized standard in encryption that has been tested and widely adopted.

9. As to claim 4, Chaney discloses wherein the broadcast signal comprises a digital television signal and the processing unit comprises a DVB circuit (col. 3, lines 39-46).

10. As to claim 5, Chaney discloses wherein the input interface has a separate input for the encrypted common key connected to the decryption circuit (col. 3, lines 57-67 to col. 4, lines 1-5, col. 1, lines 59-67, col. 5, lines 25-67).

11. As to claim 6, Chaney doesn't explicitly disclose wherein the secret key is unique to the semiconductor integrated circuit. However, Mills discloses wherein the secret key is unique to the semiconductor integrated circuit (col. 11, lines 30-50).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Chaney as taught y Mills in order to increase the security of broadcasted data that transmitted over the public network.

12. As to claims 14 and 17, these are rejected using the same rationale as for the rejection of claim 6.

13. As to claim 7, Chaney discloses wherein the common key store is arranged to store multiple common keys (col. 6, lines 65-67).

14. As to claim 11, 15, 18 and 20, these are rejected using the same rationale as for the rejection of claim 7.

15. As to claim 8, Chaney discloses a television decoder comprising the semiconductor integrated circuit of claim 1 (col. 2, lines 17-30).

16. As to claim 9, the combination of Chaney and Mills disclose a system for broadcasting signals to a plurality of subscribers in which only authorized recipients are able to decrypt the broadcast signals, the system comprising: a transmitter arranged to broadcast: signals encrypted according to control words; control words encrypted according to a common key common to two or more authorized recipients; and a common key encrypted respectively according to a unique secret key of each authorized recipient; the system further comprising a plurality of receivers, each comprising a semiconductor integrated circuit according to claim 1, wherein the secret key is unique to each semiconductor integrated circuit (Mills: col. 11, lines 30-50).

17. As to claim 12, the combination of Chaney and Mills disclose wherein the decryption device is formed as a single semiconductor integrated circuit having an input interface for receipt of encrypted broadcast signals, encrypted control signals, and encrypted common keys, and an output interface for output of decrypted broadcast signals (Mills: col. 11, lines 30-50).

18. As to claim 21, it is rejected using the same rationale as for the rejection of claim 12.

19. **Examiner's note:** Examiner has cited particular columns and line numbers in the references as applied to the claims above for the convenience of the Applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may be applied as well. It is respectfully requested from the Applicant, in preparing the responses, to fully consider the references in entirety as potentially teaching all or part of the claimed invention as well as the context of the passage as taught by the prior art or disclosed by the Examiner.

Response to Arguments

20. Applicant's arguments filed July 19, 2007 have been fully considered but they are not persuasive.

Regarding claim 1, Applicant argues that: "If one interprets Chaney in view of column 11, lines 15-20 it seems that this document does disclose ECM data (i.e. control signals) being broadcast in encrypted from and that a key (a common key as we mean it), provided on the smartcard, is needed to decrypt the ECM data. Therefore, Chaney discloses a common key being provided on the smartcard but does not disclose a system for receiving common keys provided by broadcast."

In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., "a system for receiving common keys provided by broadcast") are not recited in the

rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993). It should be noted that Examiner's job is to examine the claims as they stand without reading into the claims. According to claim 1, control signals are decrypted in accordance with a common key form a common key store in the integrated circuit. No where in claim 1 was recited that the common key was provided by broadcast. The examiner asserts with reasonable interpretation that the common key being provided on the smartcard.

Applicant argues that: "Mills does not provide the feature of the only route to placing the common key in the common key store being to input the common key in encrypted form for decryption in accordance with a secret key and provide it to the common key store over an internal."

Examiner maintains that: Chaney discloses common key store in the integrated circuit (col. 5, lines 25-67 and col. 6, lines 55-67). Furthermore, Mills discloses common key was provided in an encrypted form (Mills teaches this concept by provided service key in encrypted form) and common key is encrypted using secret key wherein secret key is stored in the smartcard (Mills teaches discloses wherein the smartcard stores a secret key for the processing system key and uses the secret key to decrypt an encrypted service key) (e.g. see, col. 11, lines 43-50).

Applicant argues that: "there is no teaching or suggestion in either Mills or Chaney, taken alone or in any combination thereof, o having both the common key store and the secret key store formed in the same integrated circuit.

Examiner maintains that: Chaney teaches a common key store in the integrated circuit (col. 5, lines 25-67 and col. 6, lines 55-67) and Mills teaches discloses wherein the smartcard stores a secret key for the processing system key and uses the secret key to decrypt an encrypted service key (e.g. see, col. 11, lines 43-50).

Conclusion

21. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

- Patent No.: US 7,165,180 B1 (Ducharme)
- Patent No. : US 5,991,400 (Kamperman)
- Patent No.: US 6,577,734 B1

22. Any inquiry concerning this communication or earlier communications from the examiner should be directed to SUMAN DEBNATH whose telephone number is (571)270-1256. The examiner can normally be reached on 8 am to 5 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Y. Vu can be reached on 571 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/S. D./
Examiner, Art Unit 2135
/Kimyen Vu/
Supervisory Patent Examiner, Art Unit 2435